

# [NT] WinHKI Directory traversal

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00062.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 22 Mar 2006 09:50:26 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

WinHKI Directory traversal

---

## SUMMARY

<<http://www.winhki.com/en/index.htm>> WinHKI is a "professional archiver and data; file compression tool for your files. WinHKI make your data very small". A directory traversal vulnerability in WinHKI allows attackers to cause the program to overwrite existing sensitive files on the system.

## DETAILS

Vulnerable Systems:  
\* WinHKI version 1.6

The vulnerability is caused due to an input validation error when extracting files compressed with RAR (.rar) or TAR (.tar) or ZIP (.zip) or TAR.GZ (tar.gz). This vulnerability makes it possible to have files extracted to arbitrary locations outside the specified directory using the "../" directory traversal sequence.

Exploit:  
Use HEAP [Hamid Evil Archive Pack] that can be downloaded from:  
<<http://www.hamid.ir/tools/>> <http://www.hamid.ir/tools/>

ADDITIONAL INFORMATION

The information has been provided by <[mailto:het\\_ebadi@xxxxxxxx](mailto:het_ebadi@xxxxxxxx)> h e.

The original article can be found at:

<<http://www.hamid.ir/security/winhki.txt>>

<http://www.hamid.ir/security/winhki.txt>

The vulnerability has been previously addressed by

<<http://www.securiteam.com/windowsntfocus/5LP072KEKM.html>> WinHKI, but appears to have resurfaced.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@xxxxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxxxx)

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.